Formal Assessment of Network Security Risks with an Integrated Assessment Instrument

David P. Gilliam
Jet Propulsion Laboratory,
California Institute of Technology
David.P.Gilliam@jpl.nasa.gov

David P. Gilliam
Jet Propulsion Laboratory,
California Institute of Technology
John.C.Kelly@jpl.nasa.gov

John D. Powell
Jet Propulsion Laboratory,
California Institute of Technology
John.Powell@jpl.nasa.gov

Abstract

The National Aeronautics and Space Administration (NASA) has tens of thousands of networked computer systems and applications. Software Security is a major concern due to the risk to both controlled and non-controlled systems from potential lost or corrupted data, lost work effort, theft of information, and unavailability of systems, especially mission critical systems. The cost to NASA if mission critical systems are compromised, especially during an encounter, would be enormous if these systems were brought down or erroneous data sent to a space craft. This research examines formal verification of IT security of network aware software and systems through the creation of a security assessment instrument for the software development and maintenance life cycle. This instrument is composed of 4 parts:

- *A Vulnerability Matrix*
- *Additional Security Assessment Tools (SATs)*
- *A Property Based Testing (PBT) Tool*
- *A Flexible Modeling Framework (FMF)*

The vulnerability matrix is part of the UC Davis DOVES database containing vulnerability descriptions and the code used to exploit them. This information is used to extract properties and requirements that express potential network vulnerabilities. These properties can then be utilized by the PBT tool and the FMF.

The SATs are a collection of tools available on the Internet that can be used to test for potential weaknesses of software code. This list includes a description of each of the tools and their uses. It will be updated as additional tools become available.

The PBT tool performs formal verification of properties, including those obtained from the vulnerability matrix, at the code level. Properties are verified by slicing the code in search of the specific vulnerability properties in question.

Like the PBT tool, the FMF formally verifies properties over the system. However, the FMF performs this action at the abstract level when code may or may not yet exist.

The assessment instrument is a comprehensive set of tools that can be used individually or together to ensure the security of network aware software application and systems. Using the various tools together provide a distinct advantage. Each tool's resulting output provides feedback into the other tools. Thus, more comprehensive assessment results are attained though the leverage each tool provides to the other when they are employed in concert.

To date, the Vulnerability Matrix and SATs have been completed. The PBT tool is schedule to be completed in June of 2001. Finally, the FMF will be delivered in 2002. An ongoing effort is underway with the Multi-Mission Encryption Communication System (MECS) to pilot the usage of this security assessment instrument.

Acknowledgement

The research described in this abstract was carried out at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration.

For further information about this ongoing research, refer to http://security.jpl.nasa.gov/projects.html